AGENCY OF HUMAN SERVICES

AHS System Acquisition Standard

Jack Green

10/13/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's security control requirements for the System Acquisitions (SA-1, SA-2, SA-3, SA-4, SA-4(1), SA-5, SA-5(1), SA-5(3)) Controls.

Revision History

Date	Version	Description	Author
	.99	Draft received from HI and reviewed by Referentia	
	1.0	Created Document	AHS
8/16/2013	2.0	Document revised for VHC standards	Jack Green
10/13/2013	3.0	Procedures reviewed and adapted for VHC business processes and security requirements	Jack Green

PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health Connect's (VHC) security control requirements for the System Acquisition (SA-1, SA-2, SA-3, SA-4, SA-4(1), SA-5, SA-5(1), SA-5(3)) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

SCOPE

The scope of this standard includes the VHC and its constituent systems only

STANDARD

Resource Allocation

1. The resources required to provide security for the information system must be determined, documented, and allocated as part of the capital planning and investment control process.
2. Security must be integrated into the Capital Planning and Investment Control (CPIC) process as follows:
   - Comply with the VHC's capital asset budget planning process.
   - Follow a methodology consistent with NIST SP 800-65, OMB Circular A-11, and related memoranda and guidance.
3. Information security requirements for the information system must be included in mission/business process planning.
   - IT security priorities and requirements at the project and enterprise level must be integrated into business cases and the related OMB Exhibit 53 and Exhibit 300 documentation.
   - Business case analysis must consider how to employ and leverage existing federal and VHC components of the security architecture and standards, including common controls, before new technology control investments may be proposed.

- Exhibit 53 and Exhibit 300 must be reviewed annually for IT security consistency and compliance with all related information including, but not limited to, information in the VHC repository (e.g., dates, system criticality details including Business Area, Line of Business, Information Type, and Privacy Act).

4. Linkage must be maintained between more detailed operational budget plans and OMB Exhibit 53 and 300 to ensure accountability of resources.
5. For information system assets that are considered critical (e.g., mission critical, continuity of operations or government, critical infrastructure), VHC shall ensure the criticality designations are consistent with other reporting data (e.g., FIPS 199 system categorization, system criticality details, OMB submissions) and reflected in the Business Impact Assessments (BIA), as applicable.
6. Annual security requirements and associated tasks and resources must be addressed as listed in OMB Exhibit 53 instructions within the business cases and accounted for over the investment life cycle.
    - The security requirements and associated tasks include but are not limited to:
        i. Risk Assessment.
        ii. System Security Plan (SSP).
        iii. Security Authorization.
        iv. Reporting.
        v. Plan of Action and Milestones (POA&M) tasks and milestones.
        vi. Background screening.
        vii. Annual Contingency Plan testing.
        viii. Annual control assessments and continuous monitoring.
        ix. Architectural sequence planning.
        x. Computer security awareness and training:
            a. Annual security awareness and training / refresher training.
            b. Specialized security training / refresher training.
    - It is expected that security costs will increase throughout the Development Phase of the life cycle and then enter a relative steady state during the Operations and Maintenance (O&M) Phase.
        i. During O&M, variations of resource requirements may occur due to periodic activities (e.g., security authorization) or unexpected requirements (e.g., court decisions, changes in governing statutes).
        ii. Good planning practices and continuous monitoring must be used to prevent or reduce the likelihood of unexpected resource requirements.
    - Security requirements and resource requirements associated with significant changes for the information system must be planned and budgeted.
        i. Percentage budget figures for current year and budget year for IT security must be based on a roll-up of these resource needs.
7. A discrete line item for information security must be established in organizational programming and budgeting documentation.

8. For systems in development, the following security requirements must be line items in the project work breakdown structure with its associated resource requirements and dates:
    - FIPS 199 security categorization.
    - Risk Assessment.
    - Privacy Impact Assessment (PIA).
    - SSP.
    - POA&M tasks and milestones.
    - Contingency Plan training and testing.
    - Interconnection Security Agreements, Memoranda of Understanding/Agreement (MOU/A), and Service Level Agreements (SLAs), if applicable.
    - Security controls assessment.
    - Security Authorization.
    - Computer security awareness and training.
    - Implementation.
9. For systems in operations and maintenance, the following security requirements must be line items in the project work breakdown structure with its associated resource requirements and dates:
    - FIPS 199 security categorization review.
    - PIA, as applicable to changes and privacy requirements.
    - Risk Assessment update or revision.
    - SSP update or revision.
    - POA&M tasks and milestones.
    - Contingency Plan training, testing and revision.
    - Security controls assessment.
        i. Associated with planned configuration changes or modifications.
        ii. Associated with annual requirements for assessment.
    - Continuous monitoring.
    - Interconnection Security Agreement and MOU/MOA review and revision, if applicable.
    - Disposition Plan, if applicable.
    - Computer security awareness and training.
    - Configuration management activities and related modifications.
10. The VHC designated repository must be used and maintained as VHC's authoritative source for relevant CPIC reporting and budgetary planning.
    - CPIC data and data in the VHC repository must be consistent.
    - The VHC repository must be used to enter and maintain dates for key information system security milestones and requirements, including but not limited to the following:
        i. Risk Assessment dates.

ii. Authorization to operate date.
iii. Approved SSP date.
iv. POA&M milestone dates.

- The VHC repository must be used to maintain other key information system security data such as FIPS 199 security categorization.

Life Cycle Support

1. The information system must be managed using a system development life cycle (SDLC) methodology that includes information security considerations.
    - NIST SP 800-64, Revision 2 must be used as guidance on security considerations in the SDLC.
2. Information system security roles and responsibilities must be defined and documented throughout the SDLC.
    - Individuals having information security roles and responsibilities must be identified.

Acquisitions

1. Requirements and/or specifications must include the following, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable state laws, federal laws, Executive Orders, directives, policies, regulations, and standards.
    - Security functional requirements/specifications.
    - Security-related documentation requirements.
    - Developmental and evaluation-related assurances requirements.
2. Acquisition packages must be reviewed for compliance with all requirements in this procedure.
3. Acquisition documents (e.g., requests for proposals) for information systems, information system components, and information system services must include, either explicitly or by reference, security requirements and/or specifications that describe:
    i. Required security capabilities (i.e., security needs and, as necessary, specific security controls and other specific FISMA requirements).
    ii. Required design and development processes.
    iii. Required test and evaluation procedures.
    iv. Required documentation.
        - The level of detail required in the documentation must be based on the security categorization for the information system.
        - Documentation must address user and system administrator guidance and information regarding the implementation of the security controls in the information system.

- Documentation must include security configuration settings and related security implementation guidance.

v. Security controls must be updated under circumstances including, but not limited to, the following:
   - As new threats/vulnerabilities are identified.
   - As new technologies are implemented.

vi. Contractors' security responsibilities.

vii. Contractors' level of screening or security supervision required.

viii. Conformance to mandates of the United States Government Configuration Baseline (USGCB) for any system-level software that is to be installed and run on an Organization desktop or laptop must be adhered to.
   - The software must adhere to USGCB configuration settings.
   - Software updates must not alter USGCB configuration settings.
   - Justifications for exemptions or deviations must be documented in writing.

4. The procurement of non-standard, system-level software that is to be installed on any VHC information system must be approved.
5. OMB must be used as guidance on configuration management and acquisition requirements.
6. NIST SP 800-23 must be used as guidance on the acquisition and use of tested/evaluated IT products.
7. NIST SP 800-35 must be used as guidance when deciding on IT security services.
8. NIST SP 800-36 must be used as guidance when selecting information security products.
9. NIST SP 800-70, Revision 2 must be used as guidance on configuration settings for IT products.
10. IRS Publication 1075 must be used as guidance on Acquisitions of information system and its components when the information system is processing FTI data.
    - Exhibit 7 language, or equivalent, must be added to the contract.
    - Services using a consolidated data center must implement appropriate controls for protecting FTI data, including appropriate Service Level Agreements (SLA).

Information System Documentation

1. Administrator documentation (i.e., whether published by a vendor/manufacturer or written in-house) for the information system and constituent components must be obtained, protected as required, and made available to authorized personnel.
    - Administrator documentation must include information that describes:
        i. Secure configuration, installation, and operation of the information system.
        ii. Effective use and maintenance of the system's security features/functions.

iii. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.

2. User documentation (i.e., whether published by a vendor/manufacturer or written in-house) for the information system and constituent components must be obtained, protected as required, and made available to authorized personnel.
   - User documentation must include information that describes:
     i. User-accessible security features/functions and how to effectively use those security features/functions.
     ii. Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner.
     iii. User responsibilities in maintaining the security of the information and information system.
3. Security documentation must be updated throughout the information system's life cycle.
4. When information system documentation is either unavailable or non- existent, the following actions must be taken:
   i. Document attempts to obtain such documentation.
   ii. Recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls.

IMPORTANT INFORMATION

These procedures can be found at http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec